Anonymization Through Data Synthesis Using Generative Adversarial Networks (ADS-GAN)

Year: 2020 | Citations: 231 | Authors: Jinsung Yoon, Lydia N. Drumright, M. van der Schaar

---

Abstract

The medical and machine learning communities are relying on the promise of artificial intelligence (AI) to transform medicine through enabling more accurate decisions and personalized treatment. However, progress is slow. Legal and ethical issues around unconsented patient data and privacy is one of the limiting factors in data sharing, resulting in a significant barrier in accessing routinely collected electronic health records (EHR) by the machine learning community. We propose a novel framework for generating synthetic data that closely approximates the joint distribution of variables in an original EHR dataset, providing a readily accessible, legally and ethically appropriate solution to support more open data sharing, enabling the development of AI solutions. In order to address issues around lack of clarity in defining sufficient anonymization, we created a quantifiable, mathematical definition for “identifiability”. We used a conditional generative adversarial networks (GAN) framework to generate synthetic data while minimize patient identifiability that is defined based on the probability of re-identification given the combination of all data on any individual patient. We compared models fitted to our synthetically generated data to those fitted to the real data across four independent datasets to evaluate similarity in model performance, while assessing the extent to which original observations can be identified from the synthetic data. Our model, ADS-GAN, consistently outperformed state-of-the-art methods, and demonstrated reliability in the joint distributions. We propose that this method could be used to develop datasets that can be made publicly available while considerably lowering the risk of breaching patient confidentiality.